1.

| | |
|---|---|
| Record Nr. | UNINA9910483956703321 |
| Titolo | Theory of Cryptography : 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings / / edited by Daniele Micciancio |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010 |
| ISBN | 1-280-38567-7<br>9786613563590<br>3-642-11799-6 |
| Edizione | [1st ed. 2010.] |
| Descrizione fisica | 1 online resource (616 p.) |
| Collana | Security and Cryptology ; ; 5978 |
| Disciplina | 004 |
| Soggetti | Data encryption (Computer science)<br>Computer networks<br>Coding theory<br>Information theory<br>Computer security<br>Computer science—Mathematics<br>Algorithms<br>Cryptology<br>Computer Communication Networks<br>Coding and Information Theory<br>Systems and Data Security<br>Math Applications in Computer Science<br>Algorithm Analysis and Problem Complexity<br>Kongress.<br>Zurich (2010) |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Description based upon print version of record. |
| Nota di bibliografia | Includes bibliographical references  and author index. |
| Nota di contenuto | Parallel Repetition -- An Efficient Parallel Repetition Theorem -- Parallel Repetition Theorems for Interactive Arguments -- Almost Optimal Bounds for Direct Product Threshold Theorem -- Obfuscation |

-- On Symmetric Encryption and Point Obfuscation -- Obfuscation of Hyperplane Membership -- Invited Talk -- Secure Computation and Its Diverse Applications -- Multiparty Computation -- On Complete Primitives for Fairness -- On the Necessary and Sufficient Assumptions for UC Computation -- From Passive to Covert Security at Low Cost -- CCA Security -- A Twist on the Naor-Yung Paradigm and Its Application to Efficient CCA-Secure Encryption from Hard Search Problems -- Two Is a Crowd? A Black-Box Separation of One-Wayness and Security under Correlated Inputs -- Threshold Cryptography and Secret Sharing -- Efficient, Robust and Constant-Round Distributed RSA Key Generation -- Threshold Decryption and Zero-Knowledge Proofs for Lattice-Based Cryptosystems -- Ideal Hierarchical Secret Sharing Schemes -- Symmetric Cryptography -- A Hardcore Lemma for Computational Indistinguishability: Security Amplification for Arbitrarily Weak PRGs with Optimal Stretch -- On Related-Secret Pseudorandomness -- A Domain Extender for the Ideal Cipher -- Delayed-Key Message Authentication for Streams -- Key-Leakage and Tamper-Resistance -- Founding Cryptography on Tamper-Proof Hardware Tokens -- Truly Efficient String Oblivious Transfer Using Resettable Tamper-Proof Tokens -- Leakage-Resilient Signatures -- Public-Key Encryption Schemes with Auxiliary Inputs -- Public-Key Cryptographic Primitives Provably as Secure as Subset Sum -- Rationality and Privacy -- Rationality in the Full-Information Model -- Efficient Rational Secret Sharing in Standard Communication Networks -- Bounds on the Sample Complexity for Private Learning and Private Data Release -- Public-Key Encryption -- New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts -- Robust Encryption -- Invited Talk -- Privacy-Enhancing Cryptography: From Theory into Practice -- Zero-Knowledge -- Concise Mercurial Vector Commitments and Independent Zero-Knowledge Sets with Short Proofs -- Eye for an Eye: Efficient Concurrent Zero-Knowledge in the Timing Model -- Efficiency Preserving Transformations for Concurrent Non-malleable Zero Knowledge -- Efficiency Limitations for ?-Protocols for Group Homomorphisms -- Composition of Zero-Knowledge Proofs with Efficient Provers -- Private Coins versus Public Coins in Zero-Knowledge Proof Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the Seventh Theory of Cryptography Conference, TCC 2010, held in Zurich, Switzerland, February 9-11, 2010. The 33 revised full papers presented together with two invited talks were carefully reviewed and selected from 100 submissions.The papers are organized in topical sections on parallel repetition, obfuscation, multiparty computation, CCA security, threshold cryptography and secret sharing, symmetric cryptography, key-leakage and tamper-resistance, rationality and privacy, public-key encryption, and zero-knowledge.